УДК 621.391

Обнаружение и идентификация базовых станций сетей Интернета вещей NB-IoT

Манелис В. Б., Сладких В. А., Шатилов Д. В.,
Ашихмин А. В., Токарев А. Б.

Постановка задачи: *в последние годы активно развиваются технологии удаленного взаимодействия устройств между собой («Интернет вещей»). В частности, широкое распространение получила узкополосная беспроводная технология NB-IoT на основе LTE. Ее особенностями являются относительно низкая скорость передачи данных, допустимость большой задержки, низкое энергопотребление, большой радиус действия. Для контроля лицензируемых диапазонов частот, выявления несанкционированно работающих базовых станций (БС), проверки соблюдения частотно-территориального плана службам радиомониторинга и радиоконтроля необходимо регулярно осуществлять поиск и анализ сигналов БС NB-IoT.* ***Целью работы*** *является разработка помехоустойчивого быстродействующего алгоритмического комплекса процедур обработки сигналов для обнаружения и идентификации БС NB-IoT.* ***Новизна:*** *представлен полный комплекс процедур обнаружения и обработки сигналов БС NB-IoT, включающий прием сообщения MIB широковещательного канала и прием сообщения SIB1 совместного канала, содержащего системные идентификаторы БС. Предложенные алгоритмы оценки частотной расстройки и частотного отклика канала, обеспечивающие компромисс между помехоустойчивостью и скоростью обработки, обладают элементами новизны.* ***Результат:*** *разработан комплекс процедур обработки сигнала БС NB-IoT, который позволяет выполнить обнаружение и идентификацию БС. Для увеличения быстродействия минимизировано время анализируемой записи сигнала. Алгоритмический комплекс успешно протестирован как методом компьютерного моделирования сигналов БС NB-IoT (различные режимы частотного расположения, параметры передачи, частотные сдвиги, каналы распространения, отношения сигнал-шум), так и на реальных сигналах.* ***Практическая значимость:*** *представленный алгоритмический комплекс обнаружения и идентификации сигналов БС NB-IoT предназначен для реализации в цифровых радиоприемных устройствах радиомониторинга. В частности, он используется в российском портативном анализаторе сигналов радиосетей АРСЕНАЛ-И. Анализатор предназначен для планирования систем на этапах развертывания и ввода в эксплуатацию, анализа зон покрытия, для радиоконтроля существующих сетей с целью проверки параметров передатчиков и соответствия частотно-территориальному плану.*

Ключевые слова: *NB-IoT, базовая станция, анализатор, идентификационные параметры, синхросигнал, широковещательный канал, совместный канал, MIB, SIB1.*

Введение

Актуальным направлением развития современных технологий является концепция «Интернета вещей» IoT (Internet of Things), представляющая собой систему удаленного взаимодействия устройств между собой с помощью аппаратно-программного обеспечения. Для межмашинных коммуникаций на большие расстояния разработан класс узкополосных энергоэффективных беспро-

Библиографическая ссылка на статью:
Манелис В. Б., Сладких В. А., Шатилов Д. В., Ашихмин А. В., Токарев А. Б. Обнаружение и идентификация базовых станций сетей Интернета вещей NB-IoT // Системы управления, связи и безопасности. 2025. № 2. С. 18-38. DOI: 10.24412/2410-9916-2025-2-018-038

Reference for citation:
Manelis V. B., Sladkikh V. A., Shatilov D. V., Ashihmin A. V., Tokarev A. B. Detection and identification of base stations of NB-IoT Internet of Things networks. *Systems of Control, Communication and Security*, 2025, no. 2, pp. 18-38 (in Russian). DOI: 10.24412/2410-9916-2025-2-018-038

водных сетей связи LPWAN (Low-power Wide-area Network). Особенностями таких сетей является относительно низкая скорость передачи данных, допустимость большой задержки, низкое энергопотребление, большой радиус действия. Существует множество стандартов и протоколов сетей LPWAN, в частности LTE-M, NB-IoT, LoRaWAN, Sigfox, Weightless, NB-Fi, XNB и др. В настоящее время широкое распространение, в том числе в России, получил стандарт беспроводной связи Narrow-Band IoT (NB-IoT) [1, 2]. Стандарт NB-IoT многое унаследовал от LTE, в том числе особенности физической структуры радиосигнала и архитектуры сети [3]. Поэтому разворачивание сетей NB-IoT возможно без значительных изменений существующего аппаратного обеспечения.

Стандарт NB-IoT предусматривает использование лицензируемых диапазонов частот, поэтому сети NB-IoT подлежат контролю государственных радиочастотных служб. Для планирования и эксплуатации сетей, проверки соответствия требований к параметрам передатчиков, анализа зон покрытия, соблюдения частотно-территориального плана необходимо регулярно проводить анализ параметров радиосигналов базовых станций (БС) NB-IoT.

Анализаторы БС NB-IoT выпускаются ведущими мировыми производителями радиоаппаратуры, в частности, Rohde & Schwarz (мобильный сканер радиосетей TSMA6B), PCTEL (сканирующий приемник IBflex), VIAVI Solutions (анализатор базовых станций CellAdvisor JD745B). Эти анализаторы зарубежного производства имеют высокую стоимость, кроме того, их свободное приобретение для российских потребителей не всегда возможно. В связи с этим разработка процедур обнаружения и идентификации сигналов БС NB-IoT и построение на этой основе отечественных анализаторов является актуальной задачей. В [4-14] представлены российские анализаторы сигналов сетей GSM, cdma2000, UMTS, LTE, 5G, DVB-T2, Wi-Fi, DMR, APCO P25 и др.

Различным вопросам приема сигналов БС NB-IoT посвящены публикации [15-23] и др. В частности, в [15-17] рассмотрены различные алгоритмы поиска и частотно-временной синхронизации, в [18-20] предложены и проанализированы варианты оценки частотного отклика канала для демодуляции. В [21] приведен пример приема сигнала БС NB-IoT, ограниченный сообщением широковещательного канала. В [22] рассматриваются варианты снижения вычислительной сложности алгоритмов обнаружения и оценки канала в приемнике, а в [23] описан вариант аппаратной реализации приема совместного канала на базе SDR-аппаратуры (Software-defined radio).

При этом полное описание алгоритмического комплекса приема сигналов БС NB-IoT, в частности, получение идентификаторов системного уровня, в известной научно-технической литературе отсутствует.

В данной статье представлены помехоустойчивые быстродействующие процедуры обнаружения и идентификации сигналов БС NB-IoT. Для удобства восприятия статья дополнена описанием особенностей структуры сигнала БС NB-IoT, а также примерами обнаружения и приема реальных сигналов NB-IoT.

1. Основные термины

В таблице 1 представлен перечень основных терминов и определений, используемых в данной работе и относящихся к узкоспециализированным понятиям телекоммуникаций и обработки сигналов. Более подробное разъяснение терминов приведено в тексте статьи.

Таблица 1 – Определения, обозначения и сокращения

Термин	Определение
OFDMA	Orthogonal Frequency Division Multiple Access – технология ортогонального частотного мультиплексирования, при которой передаваемый поток данных разделяется на несколько низкоскоростных потоков, которые передаются на различных ортогональных поднесущих
Циклический префикс	Циклическое повторение окончания OFDM символа
Частотно-временная ячейка	Структурная единица технологии OFDM, представляющая собой одну поднесущую одного OFDM символа
Ресурсный блок	Группа ячеек из 12 смежных поднесущих частот
NPSS	Narrowband Primary Synchronization Signal – первичный синхросигнал
NSSS	Narrowband Secondary Synchronization Signal – вторичный синхросигнал
NRS	Narrowband Reference Signal – опорный сигнал, используемый для оценки частотного отклика канала при демодуляции
NPBCH	Narrowband Physical Broadcast Channel – широковещательный канал
NPDSCH	Narrowband Physical Downlink Shared Channel – совместный канал
MIB	Master Information Block – сообщение широковещательного канала
SIB1	System Information Block 1 – системное широковещательное сообщение, передающееся в совместном канале и содержащее системные идентификаторы соты
QPSK	Quadrature Phase Shift Keying – квадратурная фазовая манипуляция
Опорные ячейки	Частотно-временные ячейки опорного сигнала
CRC	Cyclic redundancy check – циклический избыточный код, используемый для проверки правильности принятых данных
Мягкие решения бит	Значения бит, принимающие произвольные действительные значения
Жесткие решения бит	Значения бит, принимающие значения 0 или 1
N_{ID}^{cell}	Идентификатор соты физического уровня
N_{fr}	Номер фрейма
L	Количество бит в сообщении SIB1

2. Особенности технологии и структура сигнала БС NB-IoT

Технология NB-IoT основана на существующем стандарте LTE, включая использование ортогонального частотного мультиплексирования OFDMA (Orthogonal Frequency Division Multiple Access) [24].

Частотно-временной ресурс системы NB-IoT состоит из совокупности элементарных ячеек, представляющих собой одну поднесущую одного OFDM символа. Сигнал БС NB-IoT по полосе занимает 12 поднесущих, расстояние между которыми 15 кГц, что соответствует одному ресурсному блоку LTE. Таким образом, ширина полосы NB-IoT составляет 180 кГц.

Стандартом предусмотрено три режима частотного расположения сигнала NB-IoT:

- внутри рабочей полосы частот LTE (In-band), при котором сигнал занимает один ресурсный блок LTE, его возможное расположение представлено в [3];
- в защитном частотном интервале сигнала LTE (Guard-band);
- автономная работа в выделенном частотном канале вне полосы LTE (Standalone).

Сигнал БС NB-IoT во времени структурирован по фреймам длительностью 10 мс. Последовательность из 1024 фреймов образует гиперфрейм. Каждый фрейм состоит из десяти сабфреймов длительностью 1 мс, сабфрейм состоит из двух слотов длительностью 0,5 мс каждый. Слот состоит из 7 OFDM-символов. В NB-IoT используется циклический префикс длительностью 5,2 мкс перед первым символом слота и 4,7 мкс перед оставшимися шестью символами.

На рис. 1 представлена временная структура сигнала NB-IoT.

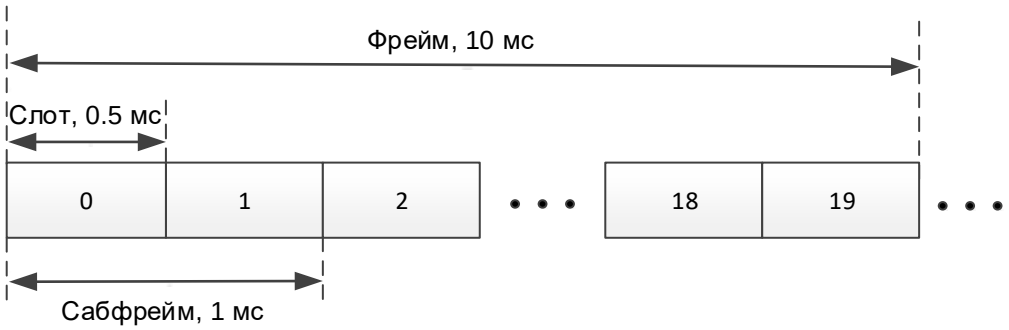


Рис. 1. Временная структура сигнала БС NB-IoT

Каждая БС сети включает в общем случае несколько сот, осуществляющих независимую передачу и прием данных в рамках своего сектора. Сигналы различных сот сети передаются одновременно в одном спектральном диапазоне. Каждая сота характеризуется идентификатором физического уровня и системными идентификаторами.

Сигнал NB-IoT соты включает совокупность различных физических каналов и сигналов [24]:

- первичный синхросигнал NPSS (Narrowband Primary Synchronization Signal);
- вторичный синхросигнал NSSS (Narrowband Secondary Synchronization Signal);
- опорный сигнал NRS (Narrowband Reference Signal);
- широковещательный канал NPBCH (Narrowband Physical Broadcast Channel);
- совместный канал NPDSCH (Narrowband Physical Downlink Shared Channel),

а также другие каналы, не используемые для обнаружения и идентификации.

Первичный синхросигнал является одинаковым для всех сот и служит для обнаружения сигнала NB-IoT и установления частотно-временной синхронизации. По вторичному синхросигналу определяется идентификатор соты физического уровня. Опорный сигнал используется для оценки частотного отклика канала при демодуляции. Совместный канал служит для передачи различных системных сообщений и трафика. Наиболее значимым является сообщение SIB1 (System Information Block 1), содержащее системные идентификаторы соты. Широковещательный канал определяет положение и параметры передачи сообщения SIB1, режим частотного расположения и другие параметры.

Расположение некоторых физических каналов и сигналов во временной области по сабфреймам показано на рис. 2.

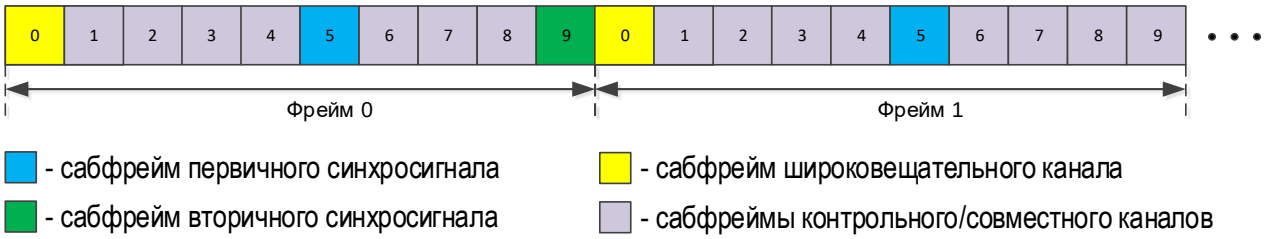


Рис. 2. Расположение некоторых физических каналов и сигналов во временной области

Стандарт NB-IoT, как и LTE, допускает возможность многоантенной передачи в режиме пространственно-частотного кодирования. При этом в NB-IoT используются две передающих антенны, в LTE – две или четыре. В этом режиме передача данных осуществляется парами символов, передаваемых на соседних поднесущих одновременно с двух различных антенн [24]. Опорный сигнал передается со всех используемых для передачи антенн. При многоантенной передаче занятые опорным сигналом ячейки не используются другими передающими антеннами.

Заметим, что в режиме In-Band в каждом сабфрейме дополнительно имеет место передача опорных символов LTE. Очевидно, соответствующие ячейки не используются сигналом NB-IoT.

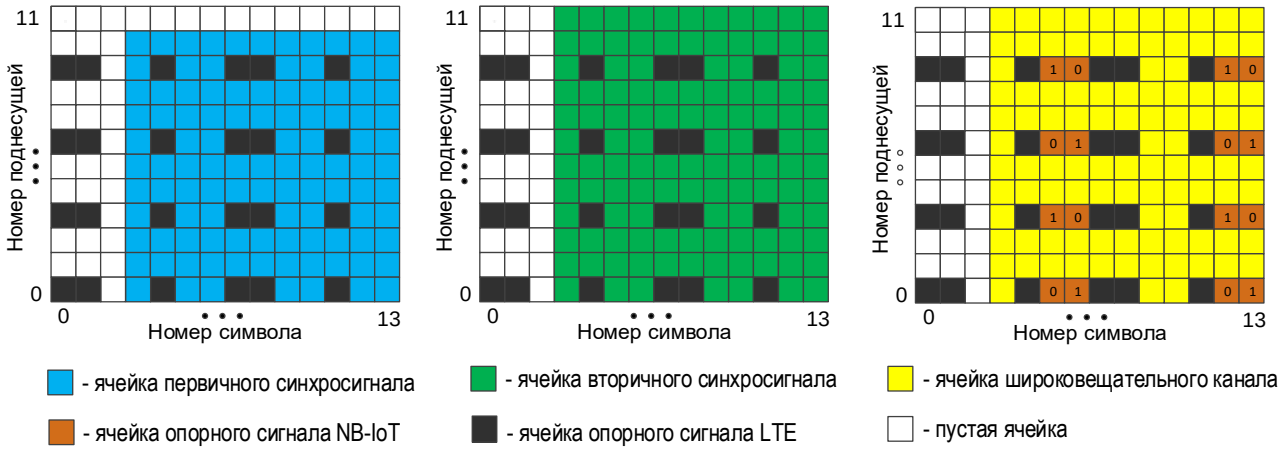
Ниже рассмотрим более подробно каналы и сигналы, прием которых необходим для решения задачи обнаружения и идентификации БС NB-IoT.

2.1. Первичный и вторичный синхросигналы

Первичный синхросигнал основан на последовательности Zadoff-Chu с хорошими корреляционными свойствами как в частотной, так и во временной областях. Как показано на рис. 2, первичный синхросигнал передается в сабфрейме 5 каждого фрейма.

Первичный синхросигнал занимает 11 поднесущих в частотной области и 11 OFDM символов во временной области соответствующего сабфрейма. В режиме In-Band ячейки, в которых передаются опорные символы LTE, для передачи первичного синхросигнала не используются. Пример сабфрейма первичного синхросигнала для режима In-Band приведен на рис. 3а.

№2. 2025
ISSN 2410-9916



а) сабфрейм первичного синхросигнала

б) сабфрейм вторичного синхросигнала

в) сабфрейм широковещательного канала для 2 антенн NB-IoT и 4 антенн LTE

Рис. 3. Примеры сабфреймов различных физических каналов и сигналов

Вторичный синхросигнал основан на m-последовательности и передается в сабфрейме 9 каждого четного фрейма. Он определяет идентификатор соты физического уровня N_{ID}^{cell}, который может принимать значения от 0 до 503. Величина N_{ID}^{cell} в режиме In-band совпадает с идентификатором физического уровня соты LTE полностью или частично.

Вторичный синхросигнал занимает 12 поднесущих в частотной области и 11 OFDM символов во временной области. В режиме In-Band ячейки, в которых передаются опорные символы LTE, для передачи вторичного синхросигнала не используются. Пример сабфрейма вторичного синхросигнала для режима In-Band приведен на рис. 3б.

2.2. Опорный сигнал

Опорный сигнал передается во всех сабфреймах, за исключением сабфреймов с первичным и вторичным синхросигналами.

Внутри сабфрейма опорный сигнал для антенн 0 и 1 передается в 6 и 7 OFDM символах каждого слота. В частотной области используются поднесущие, номера которых определяются идентификатором соты N_{ID}^{cell}. Пример возможного расположения опорных ячеек NB-IoT внутри сабфрейма для случая двухантенной передачи показан на рис. 3в.

Значения символов опорного комплексного сигнала определяются псевдослучайной последовательностью Голда длиной 31, инициируемой номером слота во фрейме и идентификатором соты N_{ID}^{cell}.

2.3. Широковещательный канал

Широковещательный канал передается в сабфрейме 0 каждого фрейма и занимает 12 поднесущих в частотной области и 11 OFDM символов во временной области. В этой частотно-временной области используются ячейки, кото-

DOI: 10.24412/2410-9916-2025-2-018-038
URL: http://sccs.intelgr.com/archive/2025-02/02-Manelis.pdf

рые не могут быть заняты опорными сигналами NB-IoT и LTE. Общее количество ячеек широковещательного канала в сабфрейме – 100. Пример сабфрейма широковещательного канала приведен на рис. 3в.

Широковещательный канал используется для передачи сообщения MIB (Master Information Block), которое передается с периодом 640 мс, состоит из 34 бит и содержит следующую основную информацию:

- 4 старших бита системного номера фрейма N_{fr};
- число повторов и размер сообщения SIB1 (4 бита);
- возможность блокировки доступа соты (1 бит);
- режим частотного расположения и некоторые параметры (7 бит).

При формировании сигнала широковещательного канала битовый блок сообщения MIB подвергается следующим процедурам [24, 25]:

- добавление к исходным 34 битам 16 проверочных бит, формируемых посредством соответствующего полинома;
- свёрточное кодирование со скоростью 1/3 с получением на выходе блока кодирования 150 бит;
- согласование скоростей для соответствия скорости передачи данных транспортного и физического каналов, которое заключается в перемежении бит, их повторе и прореживании с получением на выходе 1600 бит;
- битовое скремблирование, зависящее от идентификатора соты физического уровня;
- QPSK модуляция, при которой каждой последовательной паре бит ставится в соответствие комплексный QPSK символ, на выходе модулятора формируется 800 комплексных символов;
- распределение символов по двум потокам в случае двухантенной передачи с предварительным кодированием по схеме Аламоути;
- символьное скремблирование, зависящее от идентификатора соты физического уровня и номера фрейма;
- отображение символов модуляции на соответствующие частотно-временные ячейки сабфреймов широковещательного канала. 800 комплексных символов делятся на 8 блоков по 100 символов, каждый из которых передается восемь раз в ячейках подряд следующих сабфреймов широковещательного канала. Фрейм начала сообщения MIB удовлетворяет условию $N_{fr} \bmod 64 = 0$.

2.4. Сообщение SIB1 совместного канала

Системное сообщение SIB1, содержащее идентификаторы соты, передается в совместном канале. Сообщение SIB1 может передаваться в сабфрейме 4 каждого второго фрейма. Оно занимает 12 поднесущих в частотной области и 11 OFDM символов в режиме In-band или 14 OFDM символов в других режимах во временной области. В этих сабфреймах для передачи SIB1 используются

ячейки, которые не заняты опорными сигналами NB-IoT и LTE. Их количество может быть различным.

Сообщение SIB1 в общем случае содержит множество информационных полей. Большинство из этих полей не являются обязательными, поэтому длина сообщения SIB1 может меняться в широких пределах. Периодичность передачи сообщения SIB1 равна 2560 мс. Сообщение SIB1 содержит следующую основную информацию [25]:

- количество сетей, обслуживаемых данной сотой;
- идентификаторы сети (PLMN – Public land mobile network), MCC (Mobile Country Code), MNC (Mobile Network Code);
- идентификатор соты – CellIdentity;
- идентификатор области отслеживания внутри сети, к которой принадлежит сота – Tracking Area Code;
- доступность соты для абонентов – cellBarred.

Битовый блок SIB1 подвергается следующим процедурам для формирования сигнала [24, 25]:

- добавление к битам сообщения SIB1 24 проверочных бит, формируемых посредством соответствующего полинома;
- свёрточное кодирование со скоростью 1/3;
- согласование скоростей для соответствия скорости передачи данных транспортного и физического каналов, которое заключается в перемежении бит, их повторе и прореживании;
- битовое скремблирование, зависящее от идентификатора соты физического уровня;
- QPSK модуляция;
- распределение символов по двум потокам в случае двухантенной передачи с предварительным кодированием по схеме Аламоути;
- отображение символов модуляции на соответствующие частотно-временные ячейки сабфреймов сообщения SIB1. Символьный блок сообщения SIB1 состоит из 8 подблоков, каждый из которых передается в одном сабфрейме, так что сообщение SIB1 занимает 8 сабфреймов, передаваемых через фрейм. Каждая группа из 256 фреймов сигнала NB-IoT делится на подгруппы по 64 или 32 или 16 фреймов в соответствии с числом повторов (4 или 8 или 16). Соответствующие сабфреймы восьми первых четных фреймов каждой подгруппы заполняются символьными подблоками SIB1. Номера первых фреймов групп определяются количеством повторов и идентификатором соты N_{ID}^{cell}.

3. Обнаружение и идентификация сигнала БС NB-IoT

Частотные позиции сигнала БС NB-IoT априори неизвестны, однако сетка частот для всех возможных диапазонов известна, ее шаг составляет 100 кГц. Помимо этого в режимах In-band и Guard-band возможен дополнительный сдвиг несущей частоты на $\pm 2,5$ кГц, $\pm 7,5$ кГц [27].

№2. 2025
ISSN 2410-9916

Исходными данными для анализируемой несущей при обнаружении и идентификации БС NB-IoT является цифровой комплексный видеосигнал шириной полосы 195 кГц (с учетом возможного сдвига несущей) и частотой дискретизации $f_s = 1{,}92$ МГц. Формирование этого сигнала осуществляется в радиоприемном устройстве.

Общая схема обнаружения и идентификации сигнала БС NB-IoT представлена на рис. 4.

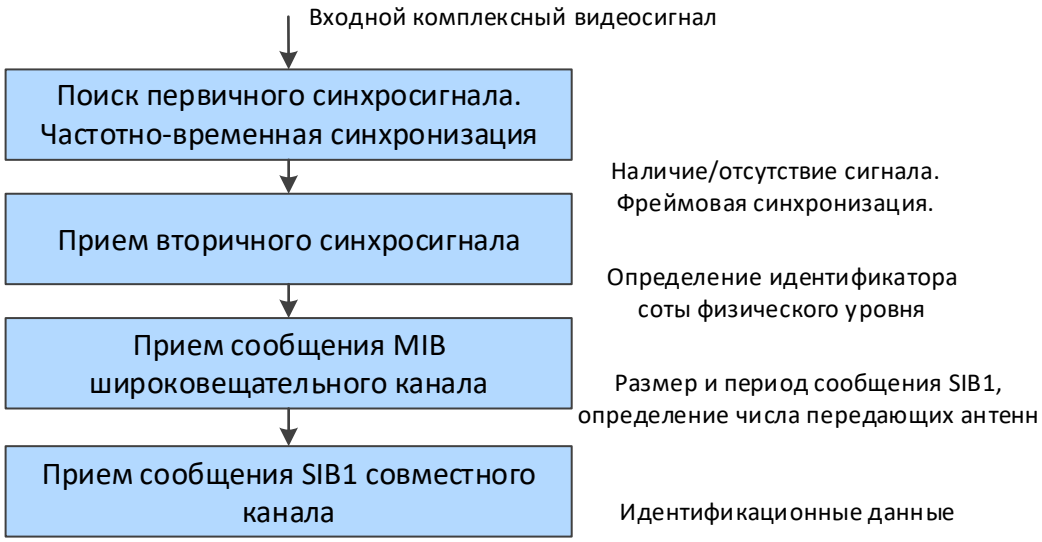


Рис. 4. Схема обнаружения и идентификации БС NB-IoT

По первичному синхросигналу выполняется обнаружение сигнала БС NB-IoT и частотно-временная синхронизация. Прием вторичного синхросигнала позволяет определить идентификатор соты физического уровня. Далее осуществляется прием сообщения MIB широковещательного канала, в котором передаются параметры передачи сообщения SIB1. После приема сообщения SIB1 извлекаются системные идентификаторы соты.

Кратко опишем необходимые процедуры.

Для обнаружения сигнала соты NB-IoT анализируется выход коррелятора, согласованного с первичным синхросигналом, на априорном интервале пяти фреймов длительностью 50 мс. Увеличенная длина интервала используется для повышения надежности обнаружения сигнала в плохих шумовых условиях. Поскольку режим частотного расположения сигнала NB-IoT априори неизвестен, выход коррелятора строится для пяти возможных вариантов частотных сдвигов 0, $\pm 2{,}5$ кГц и $\pm 7{,}5$ кГц. Если максимальное значение выходного сигнала корреляторов не превышает порог, принимается решение об отсутствии сигнала NB-IoT на анализируемой частотной несущей. В противном случае сигнал соты NB-IoT считается обнаруженным, временное положение максимума полагается началом первичного синхросигнала, а частотный сдвиг определяется по корреляторy максимума. Пример выходного сигнала коррелятора первичного синхросигнала и порога приведен на рис. 5.

DOI: 10.24412/2410-9916-2025-2-018-038
URL: http://sccs.intelgr.com/archive/2025-02/02-Manelis.pdf

№2. 2025
ISSN 2410-9916

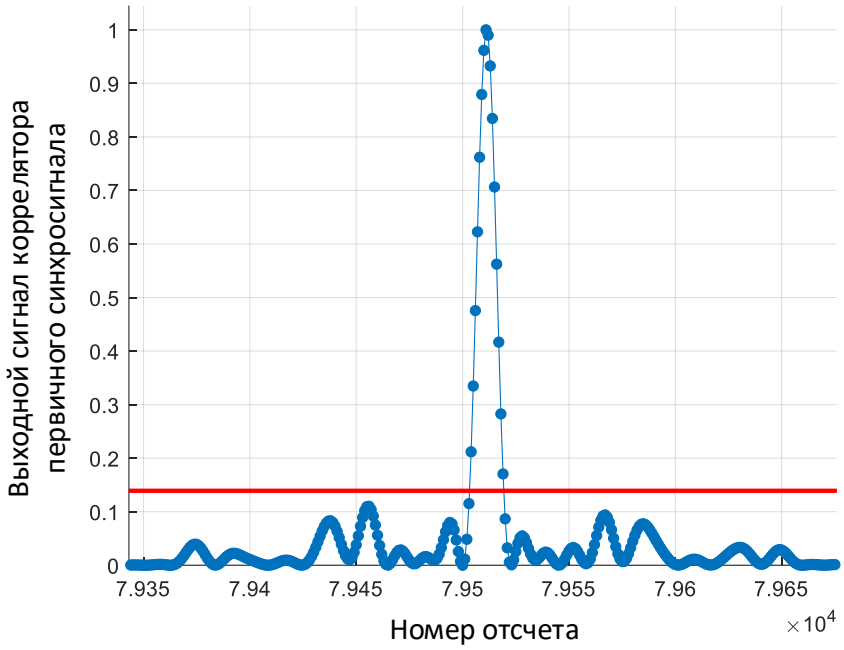


Рис. 5. Пример выходного сигнала коррелятора первичного синхросигнала (синим цветом) и порога (красным цветом)

Для оценки частотной расстройки в технологии OFDM часто применяется простой фазоразностный алгоритм, основанный на использовании префикса (повторяющихся частей символов). Однако для NB-IoT этот алгоритм показал недостаточную помехоустойчивость при низких отношениях сигнал-шум. Поэтому был использован оптимальный алгоритм с дискретным выходным сигналом, в соответствии с которым на интервале значений частотных расстроек [-800 Гц, 800 Гц] с шагом 100 Гц анализируется выход коррелятора, согласованного со сдвинутым по частоте первичным синхросигналом. По максимуму выходного сигнала коррелятора выносится оценка частотной расстройки. В соответствии с ней корректируются отсчеты входного комплексного видеосигнала. Пример выходного сигнала коррелятора показан на рис. 6. При несущественном увеличении вычислительной сложности по сравнению с фазоразностным методом реализованный алгоритм обеспечивает высокую точность оценки частотной расстройки. Рассмотрение частотных расстроек вне указанного интервала не имеет смысла, так как там наблюдается сильная деградация выходного сигнала коррелятора первичного синхросигнала, вследствие чего происходит пропуск сигнала.

Для приема вторичного синхросигнала в двух соседних фреймах для сабфреймов 9 выполняется быстрое преобразование Фурье (БПФ) длиной 128 над символами сабфреймов. Для каждого сабфрейма вычисляется корреляция между вектором результатов БПФ ячеек вторичного синхросигнала и возможными значениями этих ячеек. Истинные значения ячеек вторичного синхросигнала зависят от величины N_{ID}^{cell}, а также двух бит номера фрейма. Положение максимума рассчитанной взаимной корреляции определяет оценку идентификатора соты N_{ID}^{cell}, два бита номера фрейма, а фрейм максимума – бит его чет-

DOI: 10.24412/2410-9916-2025-2-018-038
URL: http://sccs.intelgr.com/archive/2025-02/02-Manelis.pdf

№2. 2025
ISSN 2410-9916

ности. Пример части выходного сигнала коррелятора вторичного синхросигнала, соответствующей максимуму по битам номера фрейма, приведен на рис. 7.

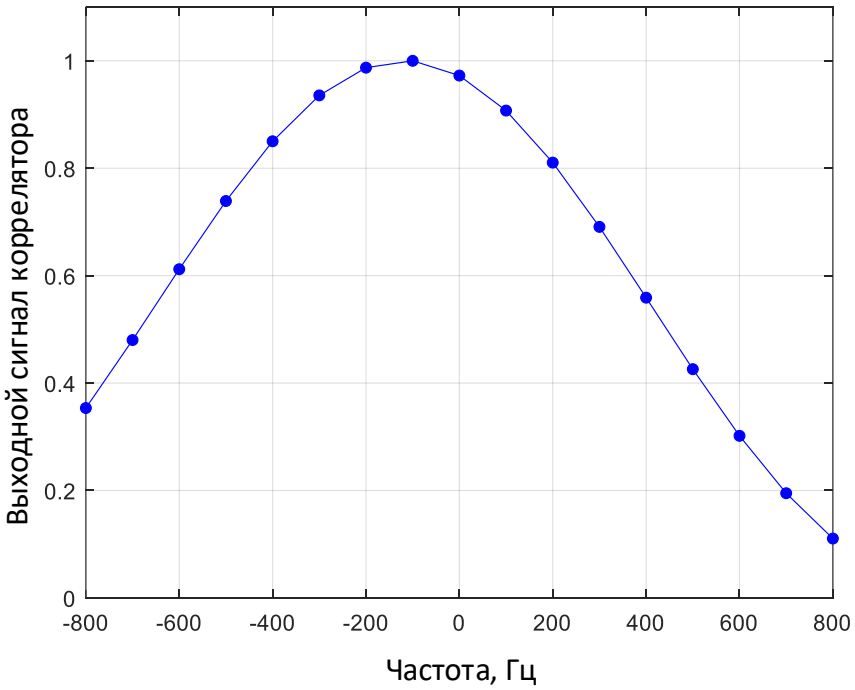


Рис. 6. Выходной сигнал коррелятора оценки частотной расстройки

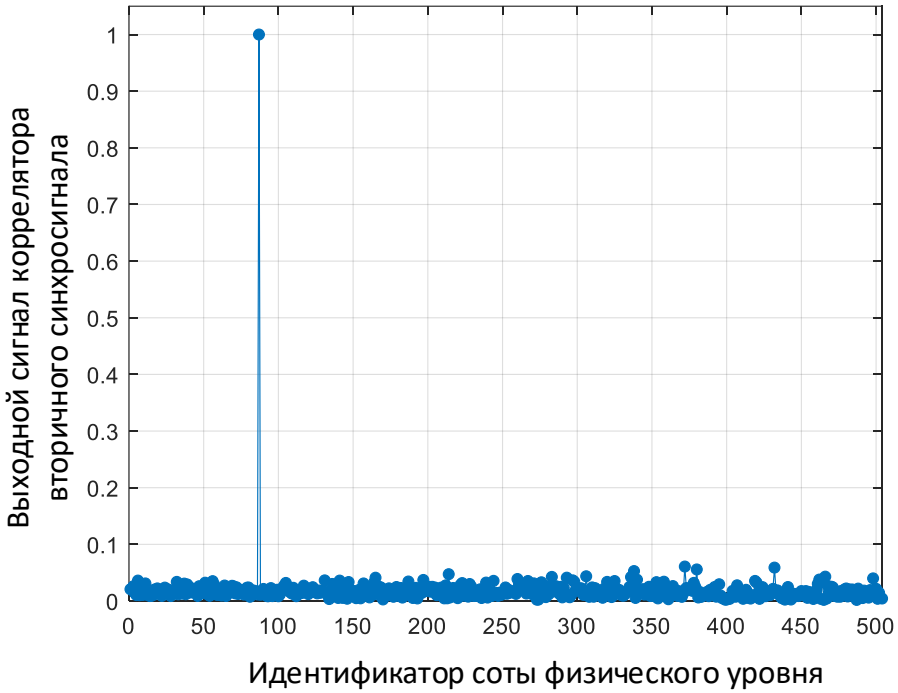


Рис. 7. Пример выходного сигнала коррелятора вторичного синхросигнала

После получения идентификатора соты физического уровня осуществляется прием сообщения MIB широковещательного канала. Общая схема процедуры приема представлена на рис. 8.

DOI: 10.24412/2410-9916-2025-2-018-038
URL: http://sccs.intelgr.com/archive/2025-02/02-Manelis.pdf

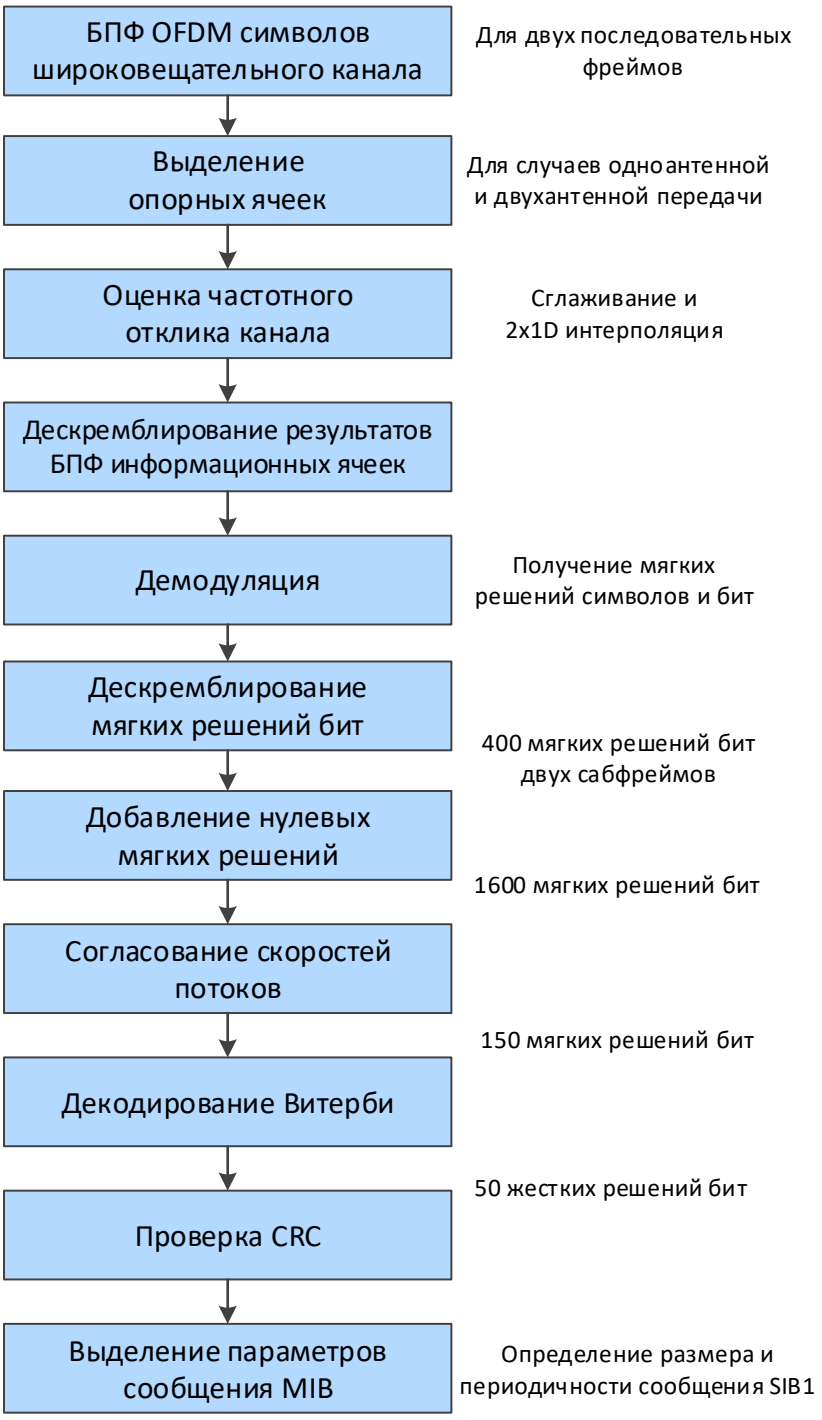


Рис. 8. Общая блок-схема приема сообщения MIB широковещательного канала

Для приема сообщения MIB используются два подряд следующих сабфрейма широковещательного канала, над символами которых выполняется БПФ длиной 128. Выбор числа используемых сабфреймов обусловлен компромиссом между скоростью обработки и помехоустойчивостью приема.

Поскольку число передающих антенн БС NB-IoT заранее не известно, процедура приема широковещательного канала в общем случае выполняется как для одноантенной, так и двухантенной передачи.

По полученному идентификатору соты N_{ID}^{cell} определяются ячейки опорного сигнала NB-IoT и их значения, а также ячейки опорного сигнала LTE.

№2. 2025
ISSN 2410-9916

Оценка частотного отклика канала для информационных ячеек каждого сабфрейма выполняется по опорным ячейкам этого сабфрейма в общем случае для двух каналов передачи. Сначала для массива значений опорных ячеек канала выполняется их сглаживание в двумерной частотно-временной области сабфрейма. По сглаженным значениям опорных ячеек методом 2×1D в два этапа интерполируются оценки канала информационных ячеек. На первом этапе для поднесущих с опорными ячейками выполняется интерполяция во временной области. На втором этапе по результатам интерполяции первого этапа осуществляется интерполяция в частотной области.

Для номера фрейма начала сообщения MIB на данном этапе приема неизвестны три бита из шести, поэтому дальнейшие процедуры выполняются в цикле из восьми вариантов предполагаемого номера фрейма.

Результат БПФ информационных ячеек широковещательного канала подвергается дескремблированию, зависящему от идентификатора N_{ID}^{cell} и предполагаемого номера фрейма.

Процедура демодуляции широковещательного канала зависит от числа передающих антенн. Для одноантенной передачи результат дескремблирования для информационной ячейки делится на оценку канала этой ячейки. Действительная и мнимая части полученной оценки символа представляют собой мягкие решения бит. При двухантенной передаче для демодуляции используется пространственно-частотное декодирование, описанное, например, в [21].

В результате демодуляции получаем массив из 400 мягких решений бит (по 200 для каждого сабфрейма). Пример мягких оценок символов широковещательного канала приведен на рис. 9. Рис. 5-7, 9 получены для успешно принятого эфирного сигнала БС NB-IoT, записанного в крупном российском городе.

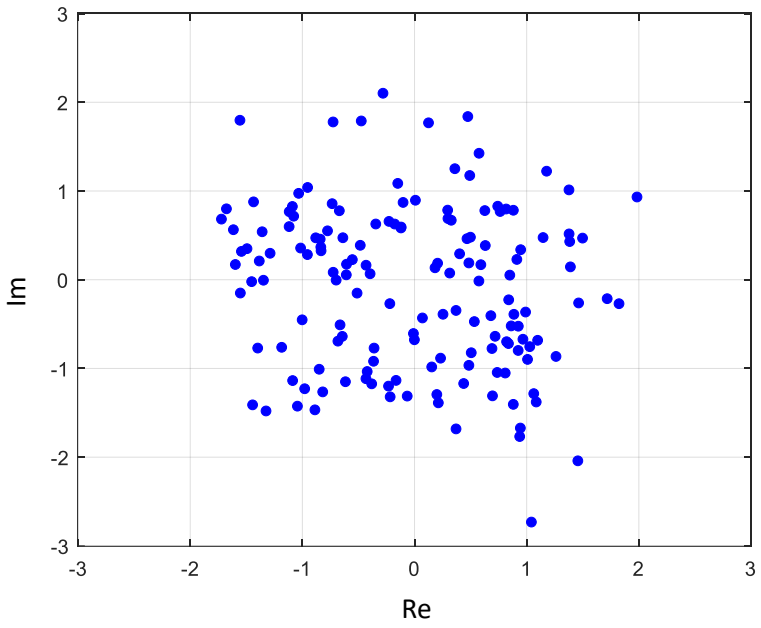


Рис. 9. Пример оценок символов широковещательного канала

DOI: 10.24412/2410-9916-2025-2-018-038
URL: http://sccs.intelgr.com/archive/2025-02/02-Manelis.pdf

Этот массив подвергается процедуре дескремблирования, которая определяется величиной N_{ID}^{cell} и предполагаемым номером фрейма.

Блок 400 дескремблированных мягких решений бит расширяется до блока размером 1600 посредством добавления нулевых мягких решений. Положение дескремблированного блока определяется предполагаемым номером фрейма.

Расширенный блок поступает на вход процедуры согласования скоростей. На выходе данной процедуры формируются 150 мягких решений бит, которые поступают на декодер Витерби, на его выходе получаем жесткие решения 50 бит.

По первым 34 битам с выхода декодера формируются 16 проверочных бит в соответствии с известным полиномом. На них накладывается маска, зависящая от числа передающих антенн. Далее сформированные и принятые проверочные биты сравниваются. Если все соответствующие биты совпадают, принимается решение о безошибочном приеме сообщения широковещательного канала. В этом случае первые 34 бита – информационные биты сообщения MIB. Кроме того, определяется число передающих антенн и фрейм начала сообщения MIB. В этом случае также выполняется выход из цикла по предполагаемому номеру фрейма.

Если какие-либо соответствующие биты не совпадают, сообщение принято с ошибкой. В этом случае делается попытка приема сообщения MIB для двух других следующих сабфреймов широковещательного канала. После заданного числа неудачных попыток работа с предполагаемой сотой прекращается.

При успешном приеме сообщения MIB окончательно определяются номера фреймов, режим частотного расположения БС, число повторов и размер сообщения SIB1 L, а также число передающих антенн LTE для режима In-Band.

Общая блок-схема приема сообщения SIB1 приведена на рис. 10. По числу повторов и идентификатору соты N_{ID}^{cell} определяется номер начального фрейма сообщения SIB1. Обработке подлежат 8 сабфреймов SIB1, передаваемые в каждом втором фрейме. Для этих сабфреймов выполняется БПФ длиной 128.

По известному числу передающих антенн для NB-IoT, а в режиме In-Band и числу передающих антенн LTE, выделяются опорные и информационные ячейки сообщения SIB1. К последним относятся все ячейки сабфрейма кроме опорных ячеек NB-IoT, а в режиме In-Band – кроме опорных ячеек NB-IoT, LTE, а также ячеек первых трех OFDM символов сабфрейма.

Оценка частотного отклика канала и демодуляция для каждого сабфрейма сообщения SIB1 выполняются аналогично соответствующим процедурам широковещательного канала.

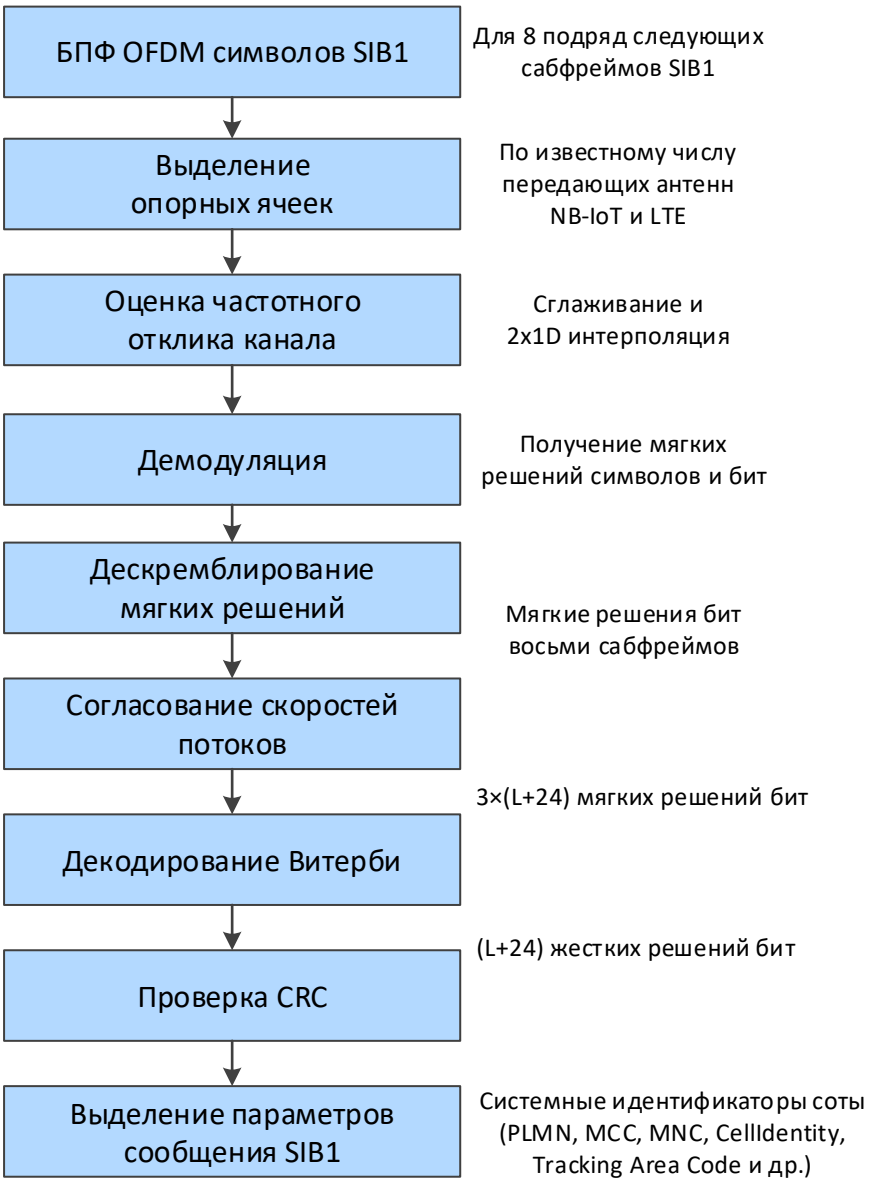


Рис. 10. Общая блок-схема приема сообщения SIB1 совместного канала

Мягкие решения информационных бит каждого сабфрейма подвергаются дескремблированию, зависящему от идентификатора N_{ID}^{cell} и номера фрейма. Дескремблированные мягкие решения восьми сабфреймов объединяются.

Объединенный блок мягких решений поступает на вход процедуры согласования скоростей, на выходе которой формируется блок $3\times\left(L+24\right)$ мягких решений бит, поступающий на декодер Витерби. На выходе декодера получаем жесткие решения $L+24$ бит.

Далее по первым L битам с выхода декодера формируются 24 проверочных бит в соответствии с известным полиномом. Выполняется сравнение 24 сформированных и принятых проверочных бит. Если какие-либо соответствующие биты не совпадают, сообщение принято с ошибкой. Если все соответствующие биты совпадают, принимается решение о безошибочном приеме транспортного блока SIB1. В результате получаем L информационных бит сообщения SIB1, из которых выделяются необходимые идентификаторы соты.

При практической реализации, кроме высокой помехоустойчивости, важной целью является повышение быстродействия работы анализатора, для чего необходима минимизация интервала анализа. Для его сокращения при приеме была существенно уменьшена используемая избыточность сообщения SIB1 и особенно MIB. В результате интервал анализа был выбран 800 мс, что позволяет иметь множество попыток приема сообщения MIB и, хотя бы одну попытку приема сообщения SIB1.

Заключение

В статье представлен помехоустойчивый быстродействующий алгоритмический комплекс процедур обнаружения и идентификации сигнала БС NB-IoT. Алгоритмический комплекс успешно протестирован как методом компьютерного моделирования сигналов БС NB-IoT для различных режимов частотного расположения, параметров передачи, частотных сдвигов, каналов распространения, отношений сигнал-шум, так и на реальных сигналах.

Представленный комплекс реализован в российском портативном анализаторе сигналов радиосетей АРСЕНАЛ-И производства АО «ИРКОС» [28]. Анализатор предназначен для планирования систем сотовой и транковой радиосвязи и передачи данных на этапах развертывания и ввода в эксплуатацию, анализа зон покрытия, а также радиоконтроля существующих сетей с целью проверки параметров передатчиков и их соответствия частотно-территориальному плану.

Литература

1. Батуев Б., Лапшин А. Стандарт NB-IoT: применение и перспективы // Беспроводные технологии. 2019. №3. С. 27-31.

2. Алексеев В. Технологии мобильной связи для IoT стандарта 3GPP Rel. 13 // Беспроводные технологии. 2016. №4. С. 44-51.

3. Kanj M., Savaux V., Le Guen M. A Tutorial on NB-IoT physical layer design // IEEE Communications Surveys & Tutorials. 2020. Vol. 20. № 4. P. 2408-2446.

4. Ашихмин А. В., Каюков И. В., Козьмин В. А., Манелис В. Б. Анализатор базовых станций GSM сетей на базе панорамного измерительного приемника АРГАМАК-ИМ // Специальная техника. 2008. № 1. С. 31-39.

5. Ашихмин А. В., Каюков И. В., Козьмин В. А., Манелис В. Б. Анализатор базовых станций CDMA сетей // Специальная техника. 2008. № 3-4. С. 16-26.

6. Алексеев П. А., Ашихмин А. В., Каюков И. В., Козьмин В. А., Манелис В. Б. Анализатор сигналов базовых станций UMTS сетей // Спецтехника и связь. 2012. № 5-6. С. 57-68.

7. Алексеев П. А., Ашихмин А. В., Беспалов О. В., Каюков И. В., Козьмин В. А., Манелис В. Б. Анализатор сигналов базовых станций GSM, UMTS, LTE сетей сотовой связи // Спецтехника и связь. 2016. № 4. С. 50-59.

8. Манелис В. Б., Козьмин В. А., Сладких В. А. Обнаружение и идентификация базовых станций сетей сотовой связи 5G // Системы управления, связи и безопасности. 2021. № 3. С. 152-178.

9. Алексеев П. А., Ашихмин А. В., Каюков И. В., Козьмин В. А., Манелис В. Б. Анализатор сигналов цифрового телевидения DVB-T2 // Спецтехника и связь. 2016. № 4. С. 15-28.

10. Беспалов О. В., Бочаров Д. Н., Каюков И. В., Козьмин В. А., Манелис В. Б. Анализатор сигналов радиостанций DMR // Спецтехника и связь. 2016. № 4. С. 106-110.

11. Ашихмин А. В., Бочаров Д. Н., Козьмин В. А., Крыжко И.Б., Козьмин В. А. Анализатор сигналов радиостанций APCO P25 // Спецтехника и связь. 2016. № 4. С. 111-114.

12. Алексеев П. А., Козьмин В. А., Крыжко И.Б., Сладких В. А. Определение параметров сетей и точек доступа Wi-Fi // Спецтехника и связь. 2016. № 4. С. 29-36.

13. Рембовский А. М., Ашихмин А. В., Козьмин В. А. Радиомониторинг – задачи, методы, средства / под ред. А.М. Рембовского. – М.: Горячая линия-Телеком, 2015. – 640 с.

14. Рембовский А. М., Ашихмин А. В., Козьмин В. А., Автоматизированные системы радиоконтроля и их компоненты / под ред. А. М. Рембовского. – М.: Горячая линия-Телеком, 2017. – 424 с.

15. Li Y., Chen S., Ye W., Lin F. A joint low-power cell search and frequency tracking scheme in NB-IoT systems for green Internet of Things // Sensors. 2018. Vol. 18. P. 1-22.

16. Ali A., Hamouda W. On the cell search and initial synchronization for NB-IoT LTE systems // IEEE communications letters. 2017. Vol. 21. P. 1843-1846.

17. Chen S., Li Y., Hunain M., Lin F. Design and implementation of cell search in NB-IoT downlink receiver // IEEE International conference on integrated circuits. 2018. P. 20-21.

18. Ali M.S., Lin F., Jewel M.K. An efficient channel estimation technique in NB-IoT systems // IEEE International conference on integrated circuits. 2018. P. 22-23.

19. Tao J., Wu J., Xiao C. Estimation of channel transfer function and carrier frequency offset for OFDM systems with phase noise // IEEE transactions on vehicular technology. 2009. Vol. 58. P. 4380-4387.

20. Hossain Jewel M.K., Zakariyya R.S., Famoriji O.J., Ali M.S., Lin F. A low complexity channel estimation technique for NB-IoT downlink system // 2019 IEEE MTT-S International Wireless Symposium. 2019. P.1-3.

21. NB-IoT Cell Search and MIB Recovery // MathWorks Documentation [Электронный ресурс]. 12.12.2024. – URL: https://www.mathworks.com/help/lte/ug/nb-iot-cell-search-and-mib-recovery.html (дата обращения 12.12.2024).

22. Zhang S., Zeng S., Ye F., Tang R., Wu P., Xia M. An efficient downlink receiver design for NB-IoT // IEEE wireless communications and networking conference. 2020. P. 1-5.

23. Abostait A., Tawfik R.M., Darweesh M., Mostafa H. Design and FPGA-based hardware implementation of NB-IoT physical uplink shared channel transmitter and physical downlink shared channel receiver // Electronics. 2023. P. 1-27.

24. 3GPP TS 36.211. LTE. Evolved Universal Terrestrial Radio Access. Physical channels and modulation. – 3GPP, 2017. – 196 с.

25. 3GPP TS 36.212. LTE. Evolved Universal Terrestrial Radio Access. Multiplexing and channel coding. – 3GPP, 2018. – 250 с.

26. 3GPP TS 36.331. LTE. Evolved Universal Terrestrial Radio Access. Radio Resource Control. Protocol specification – 3GPP, 2018. – 916 с.

27. 3GPP TS 36.108. LTE. Evolved Universal Terrestrial Radio Access. Satellite Access Node radio transmission and reception – 3GPP, 2024. – 73 с.

28. Каталог ИРКОС 2024. Автоматизированные системы и технические средства радиоконтроля [Электронный ресурс]. 2024. URL: https://www.ircos.ru/zip/cat2024.pdf (дата обращения 31.01.2024).

References

1. Batuev B., Lapshin A. Standart NB-IoT: primenenie i perspektivy [NB-Iot standard: application and prospects]. *Wireless technologies*, 2019, no. 3, pp. 27-31 (in Russian).

2. Alekseev V. Tekhnologii mobilnoy svyazi dlya IoT standarta 3GPP Rel. 13 [Mobile communication technologies for 3GPP Rel. 13]. *Wireless technologies*, 2016, no. 4, pp. 44-51 (in Russian).

3. Kanj M., Savaux V., Le Guen M. A Tutorial on NB-IoT physical layer design. *IEEE Communications Surveys & Tutorials*, 2020, vol. 20, no. 4, pp. 2408-2446.

4. Ashikhmin A. V., Kayukov I. V., Kozmin V. A., Manelis V. B. Analizator bazovykh stantsiy GSM setey na baze panoramnogo izmeritel'nogo priyemnika ARGAMAK-IM [Analyzer of base stations of GSM networks based on panoramic measuring receiver ARGAMAK-IM]. *Spetsial'naia Tekhnika*, 2008, no. 1, pp. 31-39 (in Russian).

5. Ashikhmin A. V., Kayukov I. V., Kozmin V. A., Manelis V. B. Analizator bazovykh stantsiy CDMA setey [Analyzer of CDMA base stations networks]. *Spetsial'naia Tekhnika*, 2008, no. 3-4, pp. 16-26 (in Russian).

6. Alexeev P. A., Ashikhmin A. V., Kayukov I. V., Kozmin V. A., Manelis V. B. Analizator signalov bazovykh stantsiy UMTS setey [Signal analyzer of base stations of UMTS networks]. *Specialized Machinery and Communication*, 2012, no. 5-6, pp. 57-68 (in Russian).

7. Alexeev P. A., Ashikhmin A. V., Bespalov O. V., Kayukov I. V., Kozmin V. A., Manelis V. B. Analizator signalov bazovykh stantsiy GSM, UMTS, LTE setey sotovoy svyazi [Signal analyzer of base stations GSM, UMTS, LTE cellular networks]. *Specialized Machinery and Communication*, 2016, no. 4, pp. 50-59 (in Russian).

8. Manelis V. B., Kozmin V. A., Sladkikh V. A. Obnaruzhenie i identifikatsiya bazovykh stantsiy setey sotovoy svyazi 5G [Detection and identification of base stations 5G cellular networks]. *Systems of Control, Communication and Security*, 2021, no. 3, pp. 152-178 (in Russian).

9. Alexeev P. A., Ashikhmin A. V., Kayukov I. V., Kozmin V. A., Manelis V. B. Analizator signalov tsifrovogo televideniya DVB-T2 [DVB-T2 digital television signal analyzer]. *Specialized Machinery and Communication*, 2016, no. 4, pp. 15-28 (in Russian).

10. Bespalov O. V., Bocharov D.N., Kayukov I. V., Kozmin V. A., Manelis V. B. Analizator signalov radiostantsiy DMR [DMR radio station signals analyzer]. *Specialized Machinery and Communication*, 2016, no. 4, pp. 106-110 (in Russian).

11. Ashikhmin A. V., Bocharov D.N., Kozmin V. A., Kryzhko I. B. Analizator signalov radiostantsiy APCO P25 [APCO P25 radio station signals analyzer]. *Specialized Machinery and Communication*, 2016, no. 4, pp. 111-114 (in Russian).

12. Alexeev P. A., Kozmin V. A., Kryzhko I. B., Sladkikh V. A. Opredelenie parametrov setey i tochek dostupa Wi-Fi [Determination of Wi-Fi networks and access points]. *Specialized Machinery and Communication*, 2016, no. 4, pp. 29-36 (in Russian).

13. Rembovsky A. M., Ashikhmin A. V., Kozmin V.A. *Radiomonitoring – zadachi, metody, sredstva* [Radio monitoring – tasks, methods, means]. Moscow, Hotline-Telecom, 2015. 640 p. (in Russian).

14. Rembovsky A. M., Ashikhmin A. V., Kozmin V.A. *Avtomatizirovannyye sistemy radiokontrolya i ikh komponenty* [Automated radio monitoring systems and their components]. Moscow, Hotline-Telecom, 2017. 424 p. (in Russian).

15. Li Y., Chen S., Ye W., Lin F. A joint low-power cell search and frequency tracking scheme in NB-IoT systems for green Internet of Things. *Sensors*, 2018, vol. 18, pp. 1-22.

16. Ali A., Hamouda W. On the cell search and initial synchronization for NB-IoT LTE systems. *IEEE communications letters*, 2017, vol. 21, pp. 1843-1846.

17. Chen S., Li Y., Hunain M., Lin F. Design and implementation of cell search in NB-IoT downlink receiver. *IEEE International conference on integrated circuits*, 2018, pp. 20-21.

18. Ali M.S., Lin F., Jewel M.K. An efficient channel estimation technique in NB-IoT systems. *IEEE International conference on integrated circuits*, 2018, pp. 22-23.

19. Tao J., Wu J., Xiao C. Estimation of channel transfer function and carrier frequency offset for OFDM systems with phase noise. *IEEE transactions on vehicular technology*, 2009, vol. 58, pp. 4380-4387.

20. Hossain Jewel M.K., Zakariyya R.S., Famoriji O.J., Ali M.S., Lin F. A low complexity channel estimation technique for NB-IoT downlink system. *2019 IEEE MTT-S International Wireless Symposium*, 2019, pp.1-3.

21. NB-IoT Cell Search and MIB Recovery. *MathWorks Documentation*, 12 December 2024. Available at: https://www.mathworks.com/help/lte/ug/nb-iot-cell-search-and-mib-recovery.html (accessed 12.12.2024).

22. Zhang S., Zeng S., Ye F., Tang R., Wu P., Xia M. An efficient downlink receiver design for NB-IoT. *IEEE wireless communications and networking conference*, 2020, pp. 1-5.

23. Abostait A., Tawfik R.M., Darweesh M., Mostafa H. Design and FPGA-based hardware implementation of NB-IoT physical uplink shared channel transmitter and physical downlink shared channel receiver. *Electronics*, 2023, pp. 1-27.

24. 3GPP TS 36.211. LTE. Evolved Universal Terrestrial Radio Access. Physical channels and modulation. 3GPP, 2017. 196 p.

25. 3GPP TS 36.212. LTE. Evolved Universal Terrestrial Radio Access. Multiplexing and channel coding. 3GPP, 2018. 250 p.

26. 3GPP TS 36.331. LTE. Evolved Universal Terrestrial Radio Access. Radio Resource Control. Protocol specification. 3GPP, 2018. 916 p.

27. 3GPP TS 36.108. LTE. Evolved Universal Terrestrial Radio Access. Satellite Access Node radio transmission and reception. 3GPP, 2024. 73 p.

28. IRCOS JSC Catalog. Automated systems and technical means of radio monitoring. 2024. Available at: https://www.ircos.ru/zip/cat2024.pdf (accessed 31.01.2025). (in Russian).

Статья поступила 11 марта 2025 г.

Информация об авторах

Манелис Владимир Борисович – доктор технических наук. Ведущий научный сотрудник. АО «ИРКОС». Область научных интересов: системы связи, радиомониторинг, алгоритмы приема и обработки сигналов. E–mail: vbm@ircoc.vrn.ru

Сладких Владимир Александрович – кандидат технических наук. Начальник научно-исследовательского сектора. АО «ИРКОС». Область научных интересов: радиомониторинг, цифровая обработка сигналов. E–mail: sladkihva@ircoc.vrn.ru

Шатилов Данила Владимирович – инженер-программист 3 категории. АО «ИРКОС». Область научных интересов: радиомониторинг, цифровая обработка сигналов. E–mail: shatilovdv@ircoc.vrn.ru

Ашихмин Александр Владимирович – доктор технических наук, профессор. Директор обособленного структурного подразделения. АО «ИРКОС». Область научных интересов: радиомониторинг, антенны, алгоритмы приема и обработки сигналов. E–mail: info@ircos.ru

Токарев Антон Борисович – доктор технических наук, доцент. Старший научный сотрудник научно-исследовательского сектора. АО «ИРКОС». Профессор кафедры радиотехники. Воронежский государственный технический университет. Область научных интересов: широкополосный радиоконтроль, алгоритмы цифровой обработки сигналов. E–mail: tokarevab@ircoc.vrn.ru

Адрес: 129626, Россия, г. Москва, Звездный бульвар, д. 21.

Detection and identification of base stations of NB-IoT Internet of Things networks

V. B. Manelis, V. A. Sladkikh, D. V. Shatilov,
A. V. Ashikhmin, A. B. Tokarev

Problem statement: *technologies for remote interaction of devices among themselves ("Internet of things") have been actively developing in recent years. In particular, NB-IoT wireless technology based on LTE was widespread. Its features are a relatively low data transfer rate, the permissibility of a large delay, low energy-consumption, a large radius of action. To control the licensed frequency ranges, the detection of unauthorized basic base stations (BS), checking compliance with the frequency-territorial plan for radio monitoring and radio control services, it is necessary to regute the search and analysis of the NB-IoT BS signals.* ***The aim of the work*** *is to develop a noise-resistant fast algorhythmic complex of signal processing procedures for detecting and identifying NB-IoT BS.* ***Novelty:*** *a complete set of procedures for detecting and processing signals of the NB-IoT BS is presented. It includes the receiving the message MIB of broadcasting channel and the message SIB1 of the shared channel containing the system identifiers. The proposed algorithms of the frequency offset estimation and the channel estimation, providing a compromise between noise*

resistance and digital processing speed, have the elements of novelty. ***Results:*** *a complex of signal processing procedures, which allows the detection and identification of the BS NB-IoT, has been developed. The time of the analyzed signal recording is minimized for speed increasing. The algorithmic complex is successfully tested both by the method of computer modeling (various frequency modes, transmission parameters, frequency offsets, channels, signal-noise ratio), and on real signals.* ***Practical relevance:*** *the presented algorithmic complex of detection and signal identification is designed for implementation in digital radio monitoring devices. In particular, it is used in the Russian portable radio networks analyzer Arsenal-I. The analyzer is mass-produced and successfully used for planning NB-IoT systems at the stages of deployment and commissioning, analysis of the coverage areas, for radio control of existing networks in order to check the parameters of transmitters and compliance with the frequency-territorial plan.*

Keywords: *NB-IoT, base station, analyzer, identification parameters, synchronization signal, broadcast channel, shared channel, MIB, SIB1.*

Information about Authors

Vladimir Borisovich Manelis – holder of an Advanced Doctorate in Engineering Sciences. Leading Researcher. JSC «IRCOS». Field of research: communication systems, radiomonitoring, algorithms for receiving and processing signals. E–mail: vbm@ircoc.vrn.ru

Vladimir Alexandrovich Sladkikh – Ph.D. of Engineering Sciences. Head of the Research Sector. JSC «IRCOS». Field of research: radiomonitoring, digital signal processing. E–mail: sladkihva@ircoc.vrn.ru

Danila Vladimirovich Shatilov – Engineer Programmer of third category. JSC «IRCOS». Field of research: radiomonitoring, digital signal processing. E–mail: shatilovdv@ircoc.vrn.ru

Aleksandr Vladimirovich Ashihmin – holder of an Advanced Doctorate in Engineering Sciences, Professor. Director. JSC «IRCOS». Field of research: radiomonitoring, antennas, algorithms for receiving and processing signals. E–mail: info@ircos.ru

Anton Borisovich Tokarev – Advanced Doctor of Engineering Sciences, docent. Senior Researcher at the Research sector. JSC «IRCOS». Professor of the Department of Radio Engineering. Voronezh State Technical University. Field of research: wideband radiomonitoring, digital signal processing algorithms. E–mail: tokarevab@ircoc.vrn.ru

Address: Russia, 129626, Moscow, Zvezdnyy bulvar, 21.